

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of New Hampshire

In the Matter of the Search of)

(Briefly describe the property to be searched
or identify the person by name and address))A Motorola cell phone, MODEL: A855, MEID:
A00000222EC426, and A Hewlett Packard Pavilion laptop
computer, Model: Q dv6t-2300, S/N: CNF0063S7K)

Case No. 18-mj- 230-01-AS

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of _____ New Hampshire
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before November 23, 2018 (not to exceed 14 days)
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Andrea K. Johnstone, U.S. Magistrate Judge.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 11/09/2018 4:00⁵ pm

Andrea K. Johnstone
Judge's signature

City and state: Concord, NH

Andrea K. Johnstone, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 18-mj-230-01-AJ	Date and time warrant executed: 11/14/2018 @ 12:20 PM	Copy of warrant and inventory left with: N/A - SEARCH OF SEIZED ITEMS IN HSI CUSTODY
------------------------------	--	---

Inventory made in the presence of:

HSI SPECIAL AGENT SHAWN SERRA

Inventory of the property taken and name of any person(s) seized:

— MANUAL REVIEW OF DATA ON MOTOROLA CELL PHONE, ~~PHOTOS~~ PHOTOS OF SCREENSHOTS RETAINED AS EVIDENCE BY HSI.

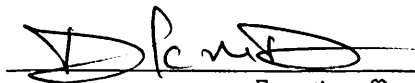
— FORENSIC EXTRACTION OF DATA OBTAINED FROM HEWLETT PACKARD PAVILLION LAPTOP, DATA RETAINED AS EVIDENCE BY HSI.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date:

12/18/2018



Executing officer's signature

SPECIAL AGENT DEREK DUNN

Printed name and title

ATTACHMENT A

The items to be searched (the DEVICES) are:

- (i) a Motorola cell phone, MODEL: A855, MEID: A00000222EC426 seized by NHSP NIU from KHAWAJA's residence pursuant to the execution of a State of New Hampshire Search Warrant on June 1, 2018; and
- (ii) a Hewlett Packard Pavilion laptop computer, Model: Q dv6t-2300, S/N: CNF0063S7K, seized by NHSP NIU from KHAWAJA's residence pursuant to the execution of a State of New Hampshire Search Warrant on June 1, 2018.

The DEVICES are currently located at HSI located at 275 Chestnut Street, Manchester, New Hampshire.

This warrant authorizes a full forensic examination of the DEVICES for the purpose of identifying, extracting and/or seizing the electronically stored information described in Attachment B.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEARCHED AND SEIZED

1. Any and all records and information on the DEVICES described in Attachment A that relate to violations of Title 21, U.S. Code, Sections 952(a), 960(a)(1), 960(b)(3), 841(a)(1) and (b)(1)(C), including, but not limited to:

- a. any and all documents, records or information associated with drug trafficking, including pay-owe sheets, buyer lists, telephone lists, address books, seller lists, ledgers, records of sales, and records of expenditures made to purchase controlled substances;
- b. any and all documents, records or information concerning types, amounts, and prices of controlled substances, as well as dates, places, and amounts of specific transactions;
- c. any and all documents, records or information related to the sources of the controlled substances, including names, addresses, phone numbers, web sites, or any other identifying information;
- d. any and all documents, records or information involving the travel to obtain controlled substances or the transportation of controlled substances;
- e. any and all documents, records or information reflecting contact or communication with coconspirators, the distribution of controlled substances to coconspirators, and the disposition of proceeds of controlled substances;
- f. any and all documents, records or information relating to the transfer, purchase, sale or disposition of virtual, digital, and cryptographic currencies and tokens (including, but not limited to, Bitcoin);
- g. any and all documents, records, or information relating to the access, creation and maintenance of websites and hidden (Tor-based) services; and
- h. any and all documents, records, or information relating to email, internet, and dark net accounts used in furtherance of these offenses;

2. Evidence of user attribution of each of the DEVICES including, but not limited to:

- a. Evidence of who used, owned, or controlled the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs,

phonebooks, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. Evidence of software that would allow others to control the DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the lack of such malicious software;

d. Evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. Evidence of the times the DEVICES was used;

g. Passwords, encryption keys, and other access devices that may be necessary to access the d DEVICES or other electronic storage media;

h. Contextual information necessary to understand the evidence described in this attachment.

3. Records and things evidencing the use of an Internet Protocol (IP) address to communicate with the internet, including, but not limited to:

a. records of Internet Protocol addresses used; and

b. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

4. Any and all hidden services accounts¹ used in furtherance of the offenses described above, including, but not limited to, Darknet market accounts, associated Darknet forum accounts and Tor-based email accounts.

¹ Hidden services (.onion services) are accessed through the Tor anonymity network. Most are considered

5. Any and all peer to peer (P2P) virtual currency trading platform accounts, with no legitimate or identified service provider to which legal process may be served, used in furtherance of the offenses described above, including, but not limited to, localbitcoins.com² accounts or bitcoin-otc internet relay chat channel³ accounts.

6. Virtual, digital, and/or cryptographic currency or tokens (hereafter, cryptocurrency) in any format, including but not limited to, wallets (digital and paper), public keys (addresses) and private keys, including, but not limited to:

- a. any and all representations of cryptocurrency public keys or addresses;
- b. any and all representations of cryptocurrency private keys, whether in electronic or physical format; and
- c. any and all representations of cryptocurrency wallets or their constitutive parts, whether in electronic or physical format, to include "root keys" which may be used to regenerate a wallet.

The United States is authorized to seize any and all cryptocurrency by transferring the full account balance in each wallet to a public cryptocurrency address controlled by the United States.

WHERE APPROPRIATE: The United States is further authorized to copy any wallet files and restore them onto computers controlled by the United States. By

dark web services with no legitimate or identified service provider to which legal process may be served.

² LocalBitcoins, OY (and their associated web platform, localbitcoins.com "LBC") is a Finnish company which is not a licensed money transmitting business registered with the U.S. Government and compliant with the Bank Secrecy Act, which requires establishment and maintenance of anti-money laundering (AML) programs in accordance with know your customer (KYC) rules, such as identifying persons involved in currency transactions over certain thresholds. LBC is not considered a legitimate service provider to which legal process may be served for accurate subscriber information or account seizure.

³ Internet Relay Chat (IRC) is a decentralized chat system which enables people with an installed client (computer program which sends and receives messages to and from an IRC server via the internet) to join in live discussions with anyone else connected in the same manner. The IRC server ensures that all messages are broadcast to everyone participating in a discussion. There can be many discussions going on at once; each one is assigned a unique channel. One such channel is #bitcoin-otc, in which virtual currency trades are negotiated and arranged. All transactions that may occur are conducted directly between counterparties, without any participation or intermediation from the hosts of IRC servers, and therefore no entity to which legal process may be served for accurate subscriber information, transactional history or account seizure.

restoring the wallets on its own computers, the United States will continue to collect cryptocurrency transferred into the defendant's wallets as a result of transactions that were not yet completed at the time that the defendant's devices were seized

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage.